REMARKS/ARGUMENTS

These remarks are in response to the Office Action dated May 26, 2005. Claims 1-29 are pending in the present application.

Claim Rejections

In the Office Action, the Examiner rejected claims 1, 3-5, 10-11, 13-15, 20-21 and 23-25 under 35 U.S.C. §103(a) as being unpatentable over Lovelace et al. (U.S. Patent No. 6,263,431) in view of Kendall (U.S. Pub. No. 2002/0144103). Claims 2, 12, and 22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Lovelace et al. (U.S. Patent No. 6,263,431), Kendall (U.S. Pub. No. 2002/0144103), and futher in view of Girard et al. (U.S. Pub. No. 2003/0061494). Claims 6, 8, 9, 16, 18, 19 26, 28 and 29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Lovelace et al. (U.S. Patent No. 6,263,431), Kendall (U.S. Pub. No. 2002/0144103), and futher in view of Jablon et al. (U.S. Patent No. 5,412,006). Claims 7, 17 and 27 were rejected under 35 U.S.C. §103(a) as being unpatentable over Lovelace et al. (U.S. Patent No. 6,263,431), Kendall (U.S. Pub. No. 2002/0144103), Jablon et al. (U.S. Patent No. 5,412,006), and futher in view of Rosenthal (U.S. Patent No. 5,359,659).

In rejecting independent claim 1, the Examiner stated:

> Referring to claim 1:
>
> i. Lovelace et al. teach:
>
> A method for tracking a secure boot in a computer system, wherein the computer system comprises a plurality of devices (see figure 1, items 111-113, 125; and column 2, lines 55-57). The method comprise the steps of providing a secure flash memory to store expected hash values (see figure 1, item 100; and column 5, lines 55-58) and a secure interface embedded in the computer system (see figure 1, item 140; and column 2, lines 44-47); booting the computer system via BIOS (see column 4, lines 1-6); calculating a measurement value for a device of the plurality of devices booted in the computer system (see figure 3, item 320); and column 5, lines 47-48); comparing the measurement value of each of the at least one device to the expected measurement value stored in the secure flash memory (see figure 3, item 340; and column 5, lines 59-60); if

measurement values match, the integrity of the computer system is assured, and the computer is booted (see figure 2, item 350; and column 5, lines 61-62).

ii. Though Lovelace et al. teach the subject matter:

Lovelace et al. teach boot components 111-114 for booting an operating system. Lovelace et al. also mention that a loader may load some boot components from a hard disk, a network device, and from other data sources. Lovelace et al. do not explicitly mention to use PCR (platform configuration register) and shadow PCR. However, Kendall discloses a flash memory comprising registers to store configuration data (see figure 3, item 31; and paragraph [0037], lines 2-7 of Kendall).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to apply the teaching of Kendall into the method of Lovelace et al., because it's efficient to user register to store/retrieve value.

Applicants respectfully submit that the cited references fail to teach or suggest the present invention as recited in claims 1-29.

Lovelace is directed to booting an operation system in a secure manner. In Lovelace, a computer system includes a secure flash memory that stores an expected hash value that has been extracted from a digital certificate prior to booting. The digital certificate is signed by a trusted authority, e.g., by an operating system vendor or hardware vendor or certificate authority. During a boot sequence, a computed hash value is computed using each of the boot components. An ordered list is used to determine the order that the boot components are supplied to the hash function to generate the computed hash value. (Col. 5, lines 46-50). The expected hash value is accessed and the computed hash value is then compared to the expected hash value. If the hash values match, the operating system is booted. (Col. 5, lines 58-67).

Kendall is directed to storing default configuration data in a non-volatile register so that a user can select between the default configuration data and a programmable configuration data. The selected configuration data is then loaded into a volatile register until a reset operation is performed. (¶ 0013 and ¶0037).

Girard is directed to protecting data on a computer. A computer is provided that has a pre-operating system (pre-OS) space and an operating system-present (OS-present) space. Protected

storage is accessed from pre-OS space via a trusted platform module (TPM). Similarly, protected storage is accessed from OS-present space via the TPM. As such, from both pre-OS space and OS-present space, a computer may prevent unauthorized users from gaining access to data stored in protected storage. (Abstract).

Jablon is directed to preventing execution of corrupted programs at time of system initialization, thereby enhancing system security. Programs and data comprising the system's trusted software, including all startup processes, are verified before being utilized. Methods to verify the trusted software use a hierarchy of both modification detection codes and public-key digital signature codes. The top-level codes are placed in a protectable non-volatile storage area, and are used by the startup program to verify the integrity of subsequent programs. A trusted initialization program sets a hardware latch to protect the codes in the non-volatile memory from being overwritten by subsequent untrusted programs. The latch is only reset at system restart, when control returns to the bootstrap program. Jablon also is directed to a system recovery process. (Abstract).

Rosenthal is directed to securing an existing executable software program against infection or corruption by software viruses or the like, without requiring any modification to the program's source code or any recompilation or relinking. Security routines capable of detecting the presence of any virus infection or other corruption are coupled to the program. The loading information for the program is modified so that upon any attempt to execute the program, the security routines will execute first and scan for viruses or other corruption. If any viruses or corruption are detected, execution of the program is aborted and a warning is displayed. If no viruses or corruption are found, the security routines are removed from memory and execution of the program continues normally. (Abstract).

Claims 1, 11 and 21

Lovelace in view of Kendall teaches a secure flash memory that stores an expected hash value in a non-volatile register, where the expected hash value is used to ensure the integrity of the boot components.

Applicants respectfully submit that Lovelace in view of Kendall fails to teach or suggest an ESS that "includes at least one boot platform configuration register (PCR) and a shadow PCR for each of the at least one boot PCR," and extending "the measurement value for a device . . . to one of the at least one boot PCRs and to the corresponding shadow PCR." In the present invention, a trusted platform module (TPM) illustrated in FIG. 3 includes a plurality of shadow PCRs 48a' that are linked, one-to-one, to a plurality of boot PCRs 48a. During a boot sequence, measurements from each bootable component are extended to the boot PCRs 48a and to the corresponding shadow PCRs 48a'. Each shadow PCR 48a' corresponds directly to each boot PCR 48a. Upon a platform reset, the boot PCRs 48a reset to zero, but the shadow PCRs 48a' retain their respective values. Thus, if an intruder boots rogue software and/or data from a removable medium, and performs a platform reset, the boot PCR 48a values reset to zero, but the shadow PCRs 48a' do not. The ensuing boot sequence, which again measures each bootable device and extends those values to the boot PCRs 48 and shadow PCRs 48a', will result in boot PCR 48a values that differ from the shadow PCR 48a' values. This indicates that unauthorized software or another operating system was booted since the last time the trusted operating system 14 was booted and prompts the trusted operating system 14 to take measures to restore trust. (Specification, page 8, lines 4-17).

In Lovelace in view of Kendall, the expected hash value is stored in the secure memory in a non-volatile register. The computed hash value is computed and then compared against the expected hash value. (Lovelace, column 5, lines 47-60). Nothing in Lovelace or Kendall teaches

or suggests providing a shadow register for each register that stores the expected hash value. Moreover, nothing in Lovelace or Kendall teaches or suggests extending the computed hash value to *both* the register and to the corresponding shadow register (which is not taught or suggested by either reference). Indeed, this would not be possible because the expected hash value is stored in a *non-volatile* register and no other hash value could be extended into it.

Based on these reasons, Applicants respectfully submit that the combination of Lovelace and Kendall fails to teach or suggest an ESS that "includes at least one boot platform configuration register (PCR) and a shadow PCR for each of the at least one boot PCR," and extending "the measurement value for a device . . . to one of the at least one boot PCRs and to the corresponding shadow PCR," as recited in claims 1, 11 and 21. Accordingly, claims 1, 11 and 21 are allowable over Lovelace in view of Kendall. Claims 3-5, 10, 13-15, 20, and 23-25 depend on claims 1, 11 and 21, respectively, and therefore, the above arguments apply with full force. Thus, claims 3-5, 10, 13-15, 20, and 23-25 are also allowable over Lovelace in view of Kendall.

Claims 2, 12, and 22

Claims 2, 12 and 22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Lovelace, Kendall, and futher in view of Girard. Claims 2, 12 and 22 depend on claims 1, 11 and 21, respectively, and therefore, the above arguments apply with full force with regard to Lovelace in view of Kendall. Applicants respectfully submit that Girard fails to teach or suggest the features of claims 1, 11 and 21, and in particular fail to teach or suggest an ESS that "includes at least one boot platform configuration register (PCR) and a shadow PCR for each of the at least one boot PCR," and extending "the measurement value for a device . . . to one of the at least one boot PCRs and to the corresponding shadow PCR." Accordingly, claims 2, 12 and 22 are allowable over the cited references.

Claims 6, 8, 9, 16, 18, 19 26, 28 and 29

Claims 6, 8, 9, 16, 18, 19 26, 28 and 29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Lovelace, Kendall, and futher in view of Jablon. Claims 6, 8,, 9, 16, 18, 19 26, 28 and 29 depend on claims 1, 11 and 21, respectively, and therefore, the above arguments apply with full force with regard to Lovelace in view of Kendall. Applicants respectfully submit that Jablon fails to teach or suggest the features of claims 1, 11 and 21, and in particular fail to teach or suggest an ESS that "includes at least one boot platform configuration register (PCR) and a shadow PCR for each of the at least one boot PCR," and extending "the measurement value for a device . . . to one of the at least one boot PCRs and to the corresponding shadow PCR." Accordingly, claims 6, 8, 9, 16, 18, 19 26, 28 and 29 are allowable over the cited references.

Claims 7, 17 and 27

Claims 7, 17 and 27 were rejected under 35 U.S.C. §103(a) as being unpatentable over Lovelace, Kendall, Jablon , and futher in view of Rosenthal. Claims 7, 17 and 27 depend on claims 1, 11 and 21, respectively, and therefore, the above arguments apply with full force with regard to Lovelace in view of Kendall. Applicants respectfully submit that Jablon and Rosenthal fail to teach or suggest the features of claims 1, 11 and 21, and in particular fail to teach or suggest an ESS that "includes at least one boot platform configuration register (PCR) and a shadow PCR for each of the at least one boot PCR," and extending "the measurement value for a device . . . to one of the at least one boot PCRs and to the corresponding shadow PCR." Accordingly, claims 7, 17 and 27 are allowable over the cited references.

Conclusion

In view of the foregoing, Applicants submit that claims 1-29 are allowable over the cited references. Applicants respectfully request reconsideration and allowance of the claims as now presented.

Applicants' attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

August 19, 2005
Date

/Joyce Tom/ Reg. No. 48,681
Joyce Tom
Attorney for Applicant(s)
Reg. No. 48, 681
(650) 493-4540